EXHIBIT B

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

[redacted] and Any Closed Containers and Electronic Devices Contained Therein

Case No. **21 MAG 9110**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
	18 U.S.C. § 1343 (wire fraud); 7 U.S.C. § 9(1) & 17 C.F.R. § 180.1(a) (insider trading in commodities); 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading in securities); 18 U.S.C. § 1348 (securities fraud); and 18 U.S.C. §§ 1956

The application is based on these facts:

See Agent Affidavit in Support of Application for Search and Seizure Warrant

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ [redacted] with permission
Applicant's signature

Special Agent [redacted]
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 09/20/2021

JAMES L. COTT
United States Magistrate Judge
Judge's signature

City and state: New York, New York

Hon. James L. Cott
Printed name and title

21 MAG 9110

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In the Matter of the Application of the United States of America for a Search and Seizure Warrant for [redacted] and Any Closed Containers and Electronic Devices Contained Therein, USAO Reference No. 2021R00875

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

[redacted], being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I am a special agent with the Federal Bureau of Investigation ("FBI") and have been so employed since approximately 2015. I am currently assigned to an FBI squad that investigates white collar crimes, including insider trading. During the course of my duties, I have received training about and participated in the execution of search warrants, and the review and analysis of both physical and electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises specified below (the "Subject Premises") for, and to seize, the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and

conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Premises

3. The Subject Premises are particularly described as [redacted]. The Subject Premises are located [redacted] and may be identified by [redacted] Based on my participation in this investigation, discussed below, I believe that Nate Chastain resides in the Subject Premises. The search warrant would authorize the search of Chastain's person at the time of the execution of the warrant to the extent Chastain is then located in the Subject Premises.

C. The Subject Offenses

4. For the reasons detailed below, I believe that there is probable cause to believe that the Subject Premises contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud); 7 U.S.C. § 9(1) & 17 C.F.R. § 180.1(a) (insider trading in commodities); 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading in securities); 18 U.S.C. § 1348 (securities fraud); and 18 U.S.C. §§ 1956 and 1957 (money laundering and money spending) (the "Subject Offenses").[1]

[1] The Commodity Exchange Act defines the term "commodity" to include several enumerated items and a catch-all for "all other goods and articles," and the Commodity Future Trading Commission has previously stated that the "commodity" definition includes cryptocurrencies such as Bitcoin and Ether, as well as renewable energy credits, emission allowances, and other intangible items. Additionally, courts have held that a digital token or coin can constitute a "security" under the Securities Act. Accordingly, while the Government's investigation as to whether the Commodity Exchange Act and the Securities Act apply to the NFTs traded on OpenSea is ongoing, there is reason to believe that such statutes potentially apply to the conduct under investigation that is discussed below.

II. Probable Cause

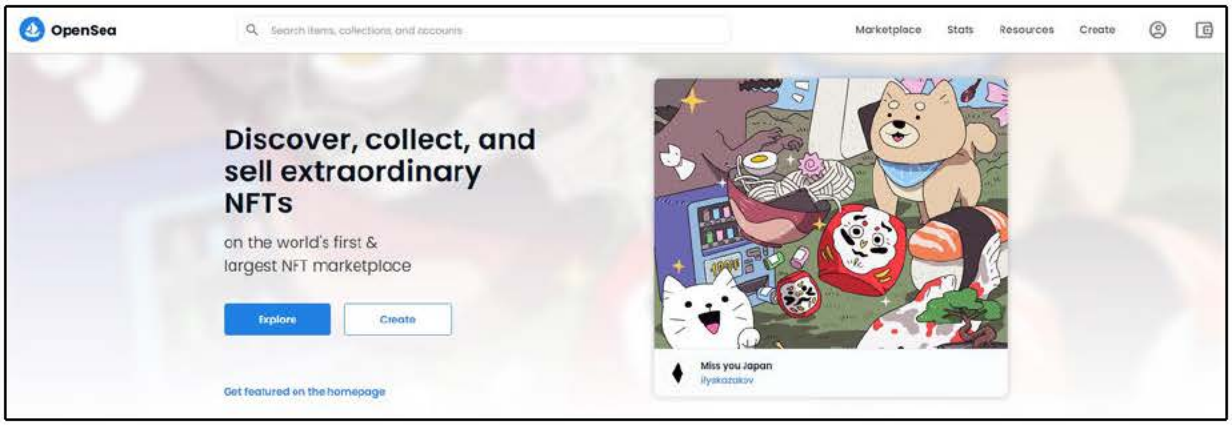
A. Probable Cause Regarding Subject's Commission of the Subject Offenses

5. The FBI and the United States Attorney's Office are investigating a scheme by Nate Chastain to trade on material non-public information obtained in the course of his employment at OpenSea, the largest trading platform for non-fungible tokens ("NFTs"). As described below, there is probable cause to believe that Chastain used non-public information about which NFTs would be featured on OpenSea to purchase those NFTs before they were featured and then sell them shortly after they were featured for a substantial profit.

6. Based on my review of publicly-available information, I have learned, among other things, the following:

a. A non-fungible token or NFT is a digital asset, based on computer code and recorded on a blockchain ledger to prove ownership and authenticity of a unique asset. NFTs can be associated with a digital or physical asset (such as a file or a physical object) and a license to use the asset for a specific purpose. Most NFTs are part of the Ethereum blockchain. Ethereum is a cryptocurrency, like bitcoin, but its blockchain (which is like a ledger) also records NFTs.

b. NFTs (and the associated license to use, copy, or display the underlying asset) can be traded and sold on digital markets. OpenSea is the largest NFT marketplace: it allows users to buy, sell, and auction NFTs and other digital items. OpenSea displays millions of NFTs and other digital items on its marketplace at a given time. OpenSea regularly features a single NFT on the front page of its website. The decision as to which NFT to feature on OpenSea's front page is made by an employee of OpenSea, and not by a computer algorithm. An example of an NFT featured on the OpenSea website is pictured below. After an NFT is featured on OpenSea's front page, its value typically appreciates substantially in a short period of time.



c. To buy or sell an NFT on OpenSea, a user needs an OpenSea account and a digital wallet. A digital wallet is software that allows a user to manage their account and "addresses" on a blockchain. An "address" in this context is a 42-character hexadecimal string that roughly corresponds to a unique location on the blockchain. NFTs are owned by an address on the blockchain, and a user, in turn, owns the address by exclusively controlling it through a private key in a digital wallet.

d. According to the terms of service that govern users' access and use of OpenSea, users are prohibited from "engag[ing] in wash trading or other deceptive or manipulative trading activities."

7. Based on my review of publicly-available information, including OpenSea's website, blockchain information, and information posted publicly by users of the OpenSea website, it appears that Nate Chastain, who was OpenSea's head of product until September 15, 2021, was purchasing NFTs based on non-public information before the NFTs were featured on OpenSea's front page, and then selling them for a profit once the price had increased due to their exposure. Specifically, I have learned the following:

a. Chastain maintained a digital wallet (with the identifier 0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) that was linked to him by his ownership

of the NFT CryptoPunk #3501. This digital wallet purchased CryptoPunk #3501 on or about February 25, 2021, and it still resides in that digital wallet's OpenSea account. Chastain's public Twitter account, @natechastain, uses CryptoPunk #3501 as its avatar, which in my training and experience is a common practice of owners of hard to acquire NFTs. Chastain's Twitter account also, as of 19 September 2021, lists "Punk #3501" in its Twitter bio, denoting ownership of this NFT. Chastain also maintained a public OpenSea account with the name "Nate", which used CryptoPunk #3501 as its avatar and linked Chastain's Twitter account @natechastain. Between approximately 3 August 2021 and 17 September 2021, the digital wallet associated with this OpenSea account named "Nate" (0x8e973de1f72ebb350c050f53abf1228934984554) sent approximately 6.6 ETH (Ethereum cryptocurrency) to Chastain's aforementioned digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D).

b. On or about August 9, 2021, at approximately 11:50 p.m. eastern time, Chastain's digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) transferred 4 ETH to an anonymous digital wallet (0x40904653ad7c8b74b777d947792ae8d7d2e8165e). Then, from approximately 11:54 p.m. on August 9 to approximately 12:00 a.m. on August 10, the anonymous digital wallet was used to purchase ten of fifty available NFTs called "Flipping and spinning" by the artist "lurk loves you" for 0.13, 0.14, 0.1425, 0.1597, 0.1999, 0.2, 0.2199, 0.22, and 0.25 ETH, respectively. At the time of the purchases, the NFT was not featured on the front page of OpenSea. Shortly thereafter, the NFT "Flipping and spinning" was featured on the front page of OpenSea. The ten NFTs were then sold for 0.42, 0.4, 0.45, 0.48, 0.5, 0.5, 0.55, 0.6, 0.65, and 0.45 ETH, respectively. Then, in two separate transactions, the anonymous digital wallet was used to send 6.07 ETH and 0.39 ETH back to Chastain's digital wallet.

c. On or about August 16, 2021, at 8:52 p.m. eastern time, a digital wallet that belongs to Chastain (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) transferred 1 ETH to an anonymous digital wallet (0x587dd0c378b02622b148afe33dabe15d5dbe6898), which then transferred 0.9988 ETH to a second anonymous digital wallet (0x13662b331eeb6629f920b63e0e193ed69b878c34). The second anonymous wallet then purchased seven of ten available NFTs called "RE-VISIT Childhood" by "gilangndaru" for 0.08 (3x) and 0.1 (4x) ETH between 9:00 p.m. and 9:05 p.m. eastern time. At the time of the purchases, the NFT was not featured on the front page of OpenSea. Shortly thereafter, the NFT "RE-VISIT Childhood" was featured on the front page of OpenSea. The NFTs were then sold between 9:10 p.m. and 9:29 p.m. for 0.4 (3x), 0.42 (2x), 0.5, and 0.6 ETH, respectively. The second anonymous digital wallet then sent 3.01 ETH back to Chastain's digital wallet.

d. On or about August 19, 2021, at 9:22 p.m. eastern time, Chastain's digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) transferred 5 ETH to an anonymous digital wallet (0x51daae200d3ecd6cbdbaf6e87cd36053e793d907). At approximately 9:25 p.m., the first anonymous digital wallet sent 4.9988 ETH to a second anonymous digital wallet (0xaa9e76c7f68d0753d4b076b772e4a59fd65a753b). Then, at approximately 9:27 p.m., the second anonymous digital wallet account sent 4.9979 ETH to a third anonymous digital wallet (0x8f11230637c4a2fd18a204ef4f13a50a049d9653). At approximately 9:45 p.m., that third anonymous digital wallet then bought five NFTs called "Focus" by "Fiidgt" for 0.12, 0.14, 0.40, 0.15, and 0.13 ETH, respectively. At the time of the purchases, the NFT was not featured on the front page of OpenSea. Shortly thereafter, the NFT "Focus" was featured on the front page of OpenSea. The NFTs were then resold for 0.62, 0.63, 0.67, 0.7, and 0.9 ETH at 9:52 p.m., 9:53

p.m., 9:59 p.m., and 10:03 p.m. The anonymous digital wallet then transferred 7.08 ETH back to Chastain's digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) at 10:07 p.m.

e. On or about August 27, 2021, at 1:17 a.m. eastern time, Chastain's digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) transferred 1 ETH to an anonymous digital wallet (0x991a6bb35fd0f3dd00c1a02065fa583a1c6049f4). At approximately 1:18 a.m., that wallet sent 0.9977 ETH to a second anonymous digital wallet (0x5f0924212dbd06a47ca47fdca66edcaba68d623b). That second wallet then bought an NFT called "tanpopoe zombie boi" by "Tanpopoe" for 0.575 ETH at 1:23 a.m. At the time of the purchases, the NFT was not featured on the front page of OpenSea. Shortly thereafter, the NFT was featured on the front page of OpenSea. At 1:30 a.m., the wallet then sold the NFT for 2.1 ETH. That wallet then sent 2.2 ETH back to Chastain's wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) at 1:35 a.m.

f. On or about September 6, 2021, at 8:38 p.m. eastern time, Chastain's digital wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D) transferred 2 ETH to an anonymous digital wallet (0xad56048cae08a93f66bef23a76f81be00044417f). At approximately 8:41 p.m., that wallet transferred 1.997 ETH to a second anonymous digital wallet (0x72de30f9e0ffe3ec0e355b042dd8bda335371bb6). At approximately 8:50 p.m., the second wallet purchased an NFT called "Happy" by "Z4". At the time of the purchases, the NFT was not featured on the front page of OpenSea. Shortly thereafter, at approximately 8:53 p.m., OpenSea's twitter account tweeted an announcement about the featured NFT. The second anonymous digital wallet then sold the same NFT at 10:59 p.m. for 1.5 ETH. That wallet then sent all its ETH (2.32 ETH) back to the Chastain's wallet (0xa3a4548b39DA96Eb065FF91811cA30da40431C0D).

g. On or about September 14, 2021, several OpenSea users made posts on Twitter calling into question whether Chastain was engaged in insider trading or frontrunning by purchasing NFTs in advance of their being featured on OpenSea's website. On or about September 15, 2021, OpenSea disclosed publicly, in a post made by its CEO, that one of its employees "purchased items that [the employee] knew were set to display on [OpenSea's] front page before they appeared their publicly."

8. Based on the foregoing, there is probable cause to believe that Chastain had access to non-public information about which NFTs had been selected to be featured on OpenSea's website and that he used that non-public information to purchase those NFTs before they were featured. It appears that Chastain used anonymous digital wallets to disguise his purchase of the NFTs and then used those digital wallets to launder the proceeds of his insider trading back to his own digital wallet. Accordingly, there is probable cause to believe that Chastain committed violations of the Subject Offenses.

B. Probable Cause Justifying Search of the Subject Premises and Electronic Devices Contained Therein

9. For the reasons set forth below, there is probable cause to believe that evidence, fruits, and instrumentalities of the commission of the Subject Offenses will be found in the Subject Premises, which is Chastain's apartment.

10. First, there is probable cause to believe that Chastain lives at the Subject Premises. Specifically:

a. Based on information provided by OpenSea, through its outside counsel, I have learned that the residential address that OpenSea had in its files for Chastain was the address for the Subject Premises.

b. On or about September 17, 2021, I visited the building located at [redacted] and viewed the building's directory. The directory stated, in relevant part, that "Chastain, N." lived [redacted]

c. I have reviewed a YouTube interview with Chastain, dated August 10, 2021, in which, based on the presence of a bed, piano, and dresser, it appears he is being interviewed in his apartment. I have also reviewed a real estate listing for the Subject Premises, which is approximately 2.5 years old, and the images of the Subject Premises depicted in the listing appear to show the same apartment as the apartment Chastain was being interviewed from in August 2021.

11. Second, there is probable cause to believe that Chastain did work for OpenSea from the Subject Premises. Specifically:

a. Based on information provided by OpenSea, through its outside counsel, I have learned that Chastain began working at OpenSea in early 2021. Until approximately August 23, 2021, all of OpenSea's employees worked remotely. From August 23, 2021, to the present, OpenSea has had office space in New York, and Chastain worked some days in the office and some days from home.

b. Based on my review of the YouTube interview with Chastain dated August 10 and August 27, 2021, it appears that Chastain did OpenSea-related interviews from his apartment – the Subject Premises.

c. I have reviewed the Twitter account @natechastain with the display name "Nate Chastain (natec.eth)," which appears to be Chastain's Twitter account. Based on my review of the tweets posted by the account, it appears that Chastain used the account for, among other things, posting OpenSea-related information. From my review of some of those tweets, it appears that Chastain did, on occasion, tweet work-related information at approximately 12:00 a.m. to 1:00

a.m., when a person would typically be at home. Therefore, there is reason to believe that Chastain made work-related tweets from the Subject Premises.

12. Third, there is probable cause to believe that the Subject Premises contains electronic devices – including at least one computer and cellphone – that contain evidence, fruits, and instrumentalities of the Subject Offenses. Specifically:

a. Based on information provided by OpenSea, through its outside counsel, I have learned that OpenSea did not issue Chastain any electronic devices and instead he used a personal cellphone and computer to do all work related to his employment. Outside counsel for OpenSea has further stated, in sum and substance, that Chastain used two company-issued email addresses to conduct work related to OpenSea. Outside counsel also stated that following Chastain's departure from the company on or around September 15, 2021, he retained these electronic devices. Accordingly, there is probable cause to believe that Chastain has electronic devices that he used for his work with him at his apartment – the Subject Premises.

b. Based on the foregoing, as well as my training and experience, there is probable cause to believe that electronic devices in the Subject Premises contain electronic evidence of the commission of the Subject Offenses. For instance, Chastain's computer and cellphone are likely to contain OpenSea emails about, among other things, NFTs being featured or displayed on OpenSea's website. Additionally, these electronic devices are also likely to contain evidence of Chastain accessing the front page of OpenSea's webpage. In this case, trading activity that is the subject of this investigation was conducted online, and therefore evidence of it is likely to be found on electronic devices. These electronic devices are also likely to contain evidence of Chastain's use of digital wallets to purchase, sell, or transfer NFTs or Ethereum because, based on my training experience, digital wallets are only accessible through electronic devices. Electronic devices also

typically contain search, web, and internet activity, and such evidence would confirm the use of those electronic devices to make NFT purchases or transfer Ethereum. Images and videos on the electronic devices are also likely to confirm that Chastain purchased certain NFTs as images or videos of those NFTs may be saved down to a phone or computer.

c. Based on my review of Chastain's Twitter account, it appears that Chastain used electronic devices to Tweet about, among other things, OpenSea's business and, in one instance, his purchase of an NFT. Specifically, on or about August 2, 2021, OpenSea's Twitter account tweeted that OpenSea's homepage would feature an NFT by Arya Mularama. Following the announcement, a Twitter user with the handle @SeanSemola tweeted, "Looks like Nate from OS had the jump on everyone else" and posted a screenshot of Chastain's digital wallet (0x8e973de1f72ebb350c050f53abf1228934984554) purchasing the NFT called "The Brawl 2". Chastain tweeted in response from his account @natechastain, "I just wanted to secure one of these before they all disappeared tbh." However, it appears that Chastain subsequently sold the NFT for 1 ETH. Chastain's tweet response confirming his purchase of this NFT from the OpenSea account titled ""nate" associated with digital wallet (0x8e973de1f72ebb350c050f53abf1228934984554) shows his admitted ownership of that account and wallet.

d. I also know, based upon my training and experience that, like individuals engaged in any other kind of activity, individuals who engage in insider trading schemes store records and communications relating to their illegal activity on electronic devices such as cellphones, computers, and iPads or PDAs. Such records can include, for example, text and voice messages; logs of online "chats" and emails with individuals from whom they receive non-public information; and records of illegal transactions including trading records, bank records and other financial records. Individuals engaged in criminal activity often store such records in order to,

among other things, (1) keep track of contact information of relevant individuals to the criminal scheme (such as a tipping individual or victim); (2) keep a record of illegal transactions for future reference; (3) keep an accounting of illegal proceeds; and (4) store stolen data for future exploitation. I also know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to commit the crimes described in this affidavit.

13. Based on my training and experience, I also know that, where computers are used in furtherance of criminal activity, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

- Electronic files can be stored on a hard drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.
- Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on a home computer, the data contained in the file does not actually disappear, but instead remains on the hard drive, in "slack space," until it is overwritten by new data that cannot be stored elsewhere on the computer. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from a hard drive or other electronic storage media depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and computer habits.
- In the event that a user changes computers, the user will typically transfer files from the old computer to the new computer, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, discs, or portable hard drives.

14. Moreover, based on my training and experience, I know that even when a user updates or replaces an iPhone, it is often the case that the full contents of the old phone are transferred to the new phone, including any historical message, call detail and browsing history. Thus, the ability to retrieve relevant information from cellphones depend less on when the

information was first created or saved than on a particular user's device configuration, storage capacity, and cellphone habits.

15. In addition to there being probable cause to believe that computer devices and cellphone(s) will be found on the Subject Premises that contain evidence of the Subject Offenses, there is also probable cause to believe that these computer(s) and cellphone(s) constitute instrumentalities of the Subject Offenses because they were used to purchase NFTs and transfer cryptocurrency.

16. Based on the foregoing, I respectfully submit there is probable cause to believe that Chastain was engaged in the commission of the Subject Offenses, and that evidence of this criminal activity is likely to be found in the Subject Premises and on computers, cellphones, and electronic media found in the Subject Premises. Specifically, based on the foregoing, there is probable cause to believe that the following evidence, described below and in Attachments A will be found within the Subject Premises and in electronic devices in the Subject Premises:

a. Evidence relating to Chastain purchasing NFTs or other digital items on OpenSea.

b. Evidence relating to which NFTs or other digital items would be featured or displayed on OpenSea's website.

c. Evidence relating to Chastain purchasing, selling, or trading NFTs or other digital items.

d. Evidence relating to Chastain's use of digital wallets, including evidence identifying digital wallets used by or associated with Chastain.

e. Evidence relating to Chastain transferring Ethereum.

f. Evidence relating to Chastain's use of proceeds from the sale of NFTs.

g. Evidence relating to OpenSea's code of conduct, employee handbook, policies, terms, or agreements concerning the use of company information or property, employees transacting in NFTs, manipulative or deceptive trading, front running, or insider trading.

h. The location of other evidence relating to the commission of the Subject Offenses including emails reflecting registration of online accounts potentially containing evidence of the scheme.

i. Evidence of user attribution showing who used or owned any device or account at any time relevant to the Subject Offenses, and dates and times any electronic device or account was used to the extent relevant to the commission of the Subject Offenses, including logs, saved usernames and passwords, browser history, search history, internet protocol records, and internet activity records.

17. Time Limitation. To the extent materials are dated, this warrant is limited to materials created, modified, sent, or received between January 1, 2021, to the present because Chastain, according to counsel for OpenSea, began working for OpenSea in 2021.

III. Procedures for Searching ESI

A. Execution of Warrant for ESI

18. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

- First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

- Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

- Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

- Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

B. Unlocking Cellphone and Tablet Devices with Biometric Features

19. I further request authority to allow law enforcement agents to obtain from the person of Chastain (but not any other individuals present at the Subject Premises at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the device(s). This authority is not to compel Chastain to provide a numeric passcode. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed above, there is reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

i. Due to the foregoing, I respectfully request that the Court authorize that, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, law enforcement personnel may obtain from the aforementioned person(s) the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

C. Review of ESI

20. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency

personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

21. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

22. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

D. Return of ESI

23. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request.

Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

24. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

25. While the execution of the requested warrant will disclose the existence of this investigation to Chastain, he does not know the scope, stage, or direction of the investigation, which is ongoing. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

/s/ [redacted] with permission

[redacted]
Special Agent
Federal Bureau of Investigation

Sworn to before me on
September 20, 2021

JAMES L. COTT
United States Magistrate Judge

ATTACHMENT A

I. Premises to be Searched—Subject Premises

The premises to be searched (the "Subject Premises") are described as follows, and include all locked and closed containers found therein:

[redacted] which is located [redacted] and may be identified by [redacted]

This warrant authorizes the search of the person of Nate Chastain in the event he is located in the Subject Premises at the time the warrant is executed.

The items to be seized from the Subject Premises also include any computer devices, cellphones and storage media that may contain any electronically stored information falling within the categories set forth in Section II.A of this Attachment, including, but not limited to, desktop and laptop computers, cellphones, thumb drives, portable hard drives, discs, and personal digital assistants. In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

II. Items to Be Seized and Review of Electronically Stored Information

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

The items to be seized from the Subject Premises consist of the following evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud); 7 U.S.C. § 9(1) & 17 C.F.R. § 180.1(a) (insider trading in commodities); 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b-5 (insider trading in securities); 18 U.S.C. § 1348 (securities fraud); and 18 U.S.C. §§ 1956 and 1957 (money laundering and money spending) (the "Subject Offenses") described as follows:

1. Evidence relating to Nate Chastain purchasing non-fungible tokens ("NFTs") or other digital items on OpenSea.

2. Evidence relating to which NFTs or other digital items would be featured or displayed on OpenSea's website.

3. Evidence relating to Nate Chastain purchasing, selling, or trading NFTs or other digital items.

4. Evidence relating to Nate Chastain's use of digital wallets, including evidence identifying digital wallets used by or associated with Chastain.

5. Evidence relating to Nate Chastain transferring Ethereum.

6. Evidence relating to Nate Chastain's use of proceeds from the sale of NFTs.

7. Evidence relating to OpenSea's code of conduct, employee handbook, policies, terms, or agreements concerning the use of company information or property, employees transacting in NFTs, manipulative or deceptive trading, front running, or insider trading.

8. The location of other evidence relating to the commission of the Subject Offenses including emails reflecting registration of online accounts potentially containing evidence of the scheme.

To the extent materials are dated, this warrant authorizes the seizure of materials created, sent, received, or modified between January 1, 2021, and the present.

B. Unlocking Devices with Biometric Features

During the execution of the warrant, law enforcement personnel are authorized to obtain from Nate Chastain the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any electronic device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

C. Review of ESI

Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.